Confusing new Chinese routers in the I2P network?!

On June 1, 2020, many more than 300 new Chinese I2P routers appeared in the network. According to I2P Metrics (operated by Tokumei), there were about 200 Chinese routers recently. After June 1st, the number of routers continued to increase. There are currently around 1444 Chinese routers according to I2P Metrics in the network. It is very unusual. For three reasons, among others:

1. The Internet in China is heavily censored. This happens through the national firewall also Golden Shield. It is therefore very difficult for I2P to perform a reseed.
2. I2P is fairly unknown in China. This means that many people in China do not know about I2P.
3. The third reason is the **sudden** surge. Increase and decrease the I2P router in China. Or increasing over a longer period of time is not uncommon, but it is not normal for over 1,000 new I2P routers to appear in such a short time.

What is known about the routers?

The routers are all from China. Furthermore, as the pie charts below show, they come from the same IP address space. The Whois data also show that many of the I2P addresses are operated by the same providers (ISPs). These include “TencentCloud” and “Alisoft”, but also “Chinanet”. According to I2P developer zzz, the routers are operated on i2pd (the C++ implementation of I2P). According to information in the Netdb, the routers all use version 0.9.42. It was also found that many routers are low-capacity routers, meaning that they provide very little bandwidth. According to Netdb, many of the new routers have the cap "L". This means that they pass a maximum of 32KB per second.

The developer zzz put forward a few theories:

- That it is a real increase. For example, based on a recommendation. This would be good for the network itself.
- That they are Chinese researchers who are researching the I2P network. However, they would not have discussed this with the developers beforehand.
- That the Chinese government is attacking the I2P network. One argument is that the Chinese government is censoring the Internet and you can use I2P to escape this censorship. One argument against this is that I2P is (unfortunately) fairly unknown and is therefore not in the interest of the Chinese government.
- It could be a change in the I2P router, which came out with the version 0.9.46, which causes more I2P routers to be classified as Chinese. You

can see the diagrams below, which show which ISPs are used. You can see that they are Chinese and no others. Therefore, this is very unlikely.
- There could also be a change in the I2P router version 0.9.46, so that the "hidden" mode in I2P is switched off and you can see more Chinese I2P routers.
- A change in the I2P router version 0.9.45, which causes hidden I2P routers to integrate better into the network. The changes can only be seen now (why?).
- There could be a change in the "Golden Shield", the national firewall, which makes it difficult to use I2P in China.

It's probably a research or an attack.

What could such an attack look like?

Traffic would be routed through the "bad" I2P routers, ie those that attack. However, this would be very slow since the routers (as stated above) pass through a maximum of 32 KB per second. Furthermore, an I2P tunnel is as fast as the slowest participant.

What could you do about such an attack?

An I2P router is configured in such a way that it always builds a tunnel from very fast routers. However, if it should happen that the routers block the traffic in the I2P network, the developers could send a "blocklist" to the I2P routers, which blocks the IP addresses of the "bad" I2P routers. As a result, the I2P router would no longer establish a connection to the "bad" routers.

What has been done to determine if they are researchers?

Tokumei, an I2P researcher and the operator of I2P Metrics, posted a post on Twitter that the researchers are looking for. Sadie, zzz and others from I2P Team tweeted this tweet (some kind of share). Sadie also posted the post on Mastodon.

Komische neue chinesische Router im I2P Netzwerk?!

Am 1. Juni 2020 sind bei vielen über 300 neue chinesische I2P Router im Netzwerk aufgetaucht. Nach I2P Metrics (betrieben von Tokumei) waren es zuletzt etwa 200 chinesische Router. Nach dem 1. Juni ist die Anzahl der Router weiter gestiegen. Aktuell sind etwa 1444 chinesische Router nach I2P Metrics im Netzwerk. Dies ist sehr ungewöhnlich. Unter anderem aus drei Gründen:

1. Das Internet in China wird stark zensiert. Dies geschieht durch die nationale Firewall auch Golden Shield. Daher ist es für I2P sehr schwierig, einen Reseed durchzuführen.
2. I2P ist in China recht unbekannt. Dies bedeutet, dass viele Menschen in China I2P nicht kennen.

3. Der dritte Grund ist der starke **plötzliche** Anstieg. Das I2P Router in China mal zunehmen und abnehmen. Oder auch über einen längeren Zeitraum zunehmen, ist nicht ungewöhnlich, allerdings ist es nicht normal, dass in so kurzer Zeit über 1000 neue I2P Router auftauchen.

Was ist über die Router bekannt?

Die Router stammen alle aus China. Des Weiteren, wie die Kreisdiagramme unten zeigen, stammen sie aus dem selben IP-Adress-Raum. Die Whois Daten zeigen außerdem, dass viele der I2P Adressen von den gleichen Anbietern (ISP‘s) betrieben werden. Zu diesen gehören „TencentCloud“ und „Alisoft“, aber auch „Chinanet“. Nach I2P Entwickler zzz werden die Router auf i2pd (der C++ Implementation von I2P) betrieben. Nach Angaben in der Netdb verwenden die Router alle die Version 0.9.42. Außerdem war festzustellen, dass viele Router Low-Capacity Router sind, also sehr wenig Bandbreite zu Verfügung stellen. Nach Netdb besitzen viele der neuen Router das Cap groß „L“. Dies bedeutet, dass sie maximal 32KB pro Sekunden durchlassen.

Der Entwickler zzz stellte ein paar Theorien auf:

- Dass es ein echten Anstieg ist. Beispielsweise aufgrund einer Empfehlung. Dies wäre für das Netzwerk an sich gut.
- Dass es sich um chinesische Forscher handelt, welche das I2P-Netzwerk erforschen. Dies hätten sie dann allerdings nicht vorher mit den Entwicklern abgesprochen.
- Dass es ein Angriff auf das I2P-Netzwerk von Seiten der chinesischen Regierung ist. Ein Argument dafür ist, dass die chinesische Regierung das Internet zensiert und man I2P benutzen kann, um dieser Zensur zu entkommen. Ein Argument dagegen ist, dass I2P (leider) recht unbekannt ist und daher nicht im Interesse der chinesischen Regierung ist.
- Es könnte sich um eine Änderung im I2P Router handelt, welche mit der Version 0.9.46 herausgekommen ist, welche bewirkt, dass mehr I2P Router als Chinesisch eingestuft werden. Dazu kann man sich die Diagramme unten ansehen, welche zeigen, welche ISP‘s verwendet werden. Man erkennt, dass es chinesische sind und keine anderen. Daher ist dies recht unwahrscheinlich.
- Es könnte aber auch eine Änderung in der I2P Router Version 0.9.46 geben, sodass der „versteckte“ Modus in I2P ausgeschaltet wird und man dadurch nun mehr chinesische I2P Router sehen kann.
- Eine Änderung in der I2P Router Version 0.9.45, welche bewirkt dass sich versteckte I2P Router besser in das Netzwerk integrieren. Die Änderungen sieht man allerdings erst jetzt (Warum?).
- Es könnte eine Änderung im „Golden Shield“ handeln, also der nationalen Firewall, welche es schwierig macht, I2P in China zu benutzen.

Wahrscheinlich handelt es sich um eine Forschung oder einen Angriff.

Wie könnte ein solcher Angriff aussehen?

Durch die „bösen“ I2P Router, also die, welche angreifen, würde Traffic geleitet. Dieser wäre allerdings sehr langsam, da die Router (wie oben festgestellt) maximal 32 KB pro Sekunden durchleiten. *Des Weiteren gilt, dass ein I2P Tunnel maximal so schnell ist, wie der langsamste Teilnehmer.*

Was könnte man gegen einen solchen Angriff tun?

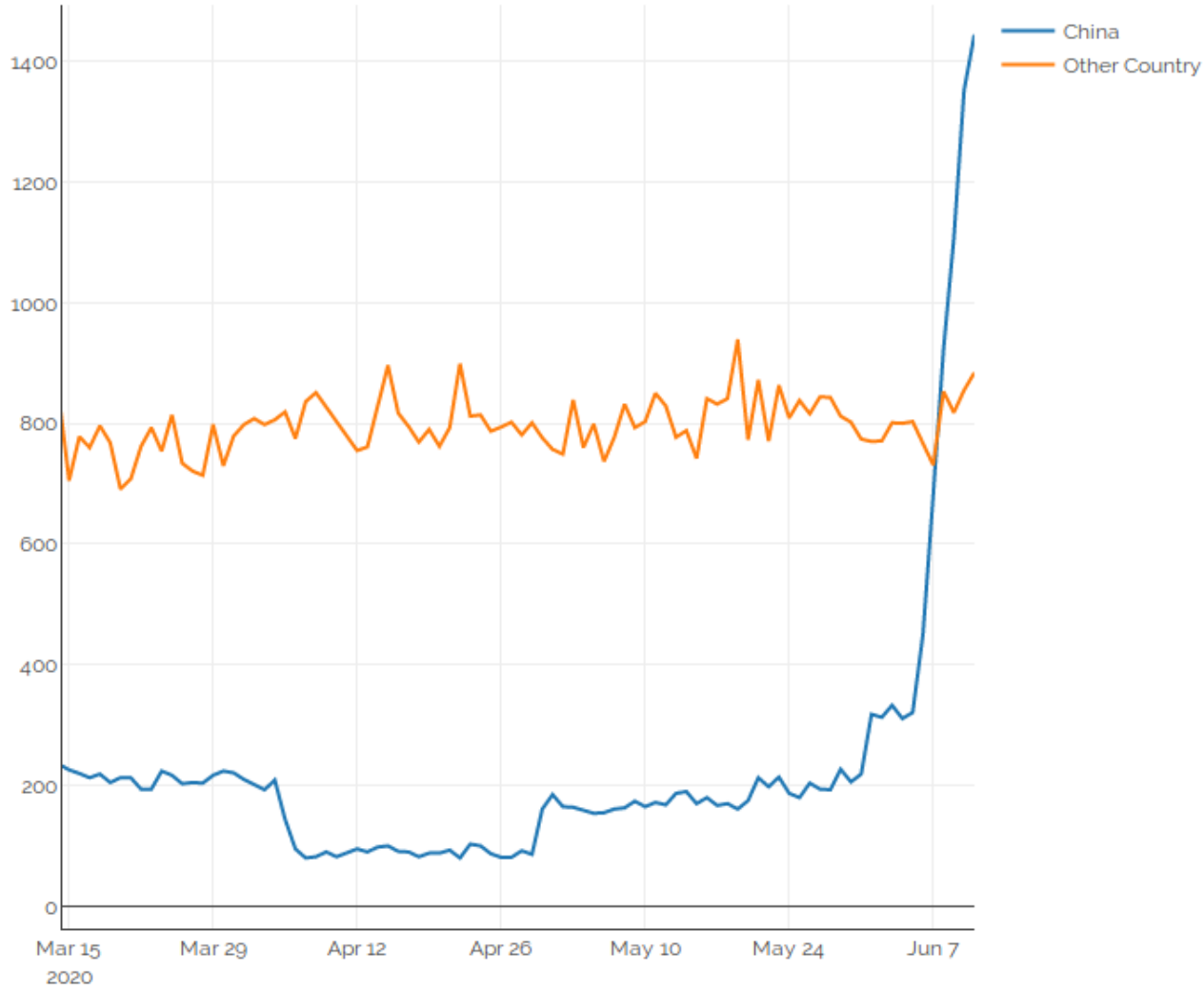
Ein I2P Router ist an sich so konfiguriert, dass er einen Tunnel immer aus sehr schnellen Routern baut. Sollte es allerdings doch so kommen, dass die Router den Verkehr im I2P Netzwerk behindern, könnten die Entwickler eine „Blocklist“ zu den I2P Routern senden, welche die IP-Adressen der „bösen“ I2P Router blockiert. Dadurch würde der I2P Router keine Verbindung mehr zu den „bösen“ Routern herstellen.

Was wurde getan, um festzustellen, ob es sich um Forscher handelt?

Tokumei, ein I2P-Forscher sowie der Betreiber von I2P Metrics, hat einen Beitrag auf Twitter gepostet, nach dem die Forscher gesucht werden. Sadie, zzz und andere von I2P Team haben diesen Tweet getweetet (eine Art von teilen). Des Weiteren wurde der Beitrag auch von Sadie auf Mastodon gepostet.

Diagrams

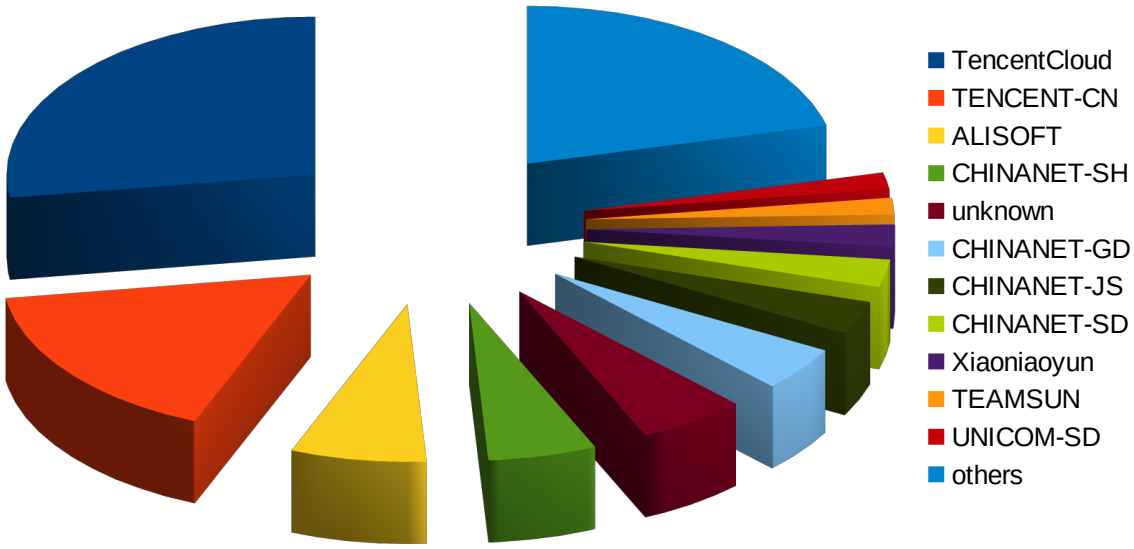
This is a diagram from I2P Metrics showing the huge slope of I2P routers in China.



Source: https://i2p-metrics.np-tokumei.net/router-distribution

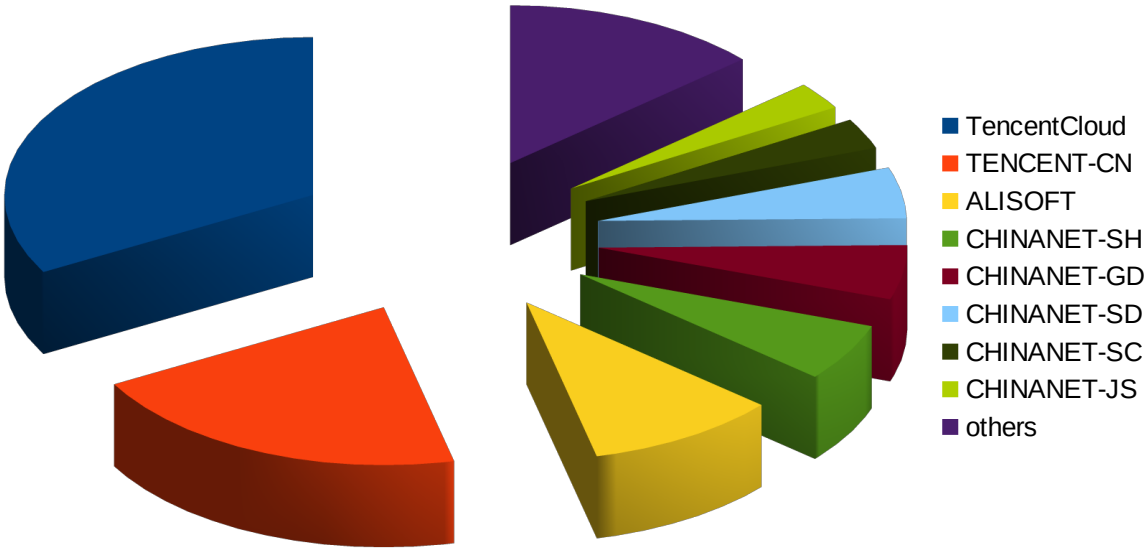
The data is based on the evaluations from my two servers, each of which operates an I2P router. In the first diagram the "Netname" is shown in the Whois. The second diagram shows the IP distribution. The ?.?.x.x means that the first two digits were the same. "others" means that they occurred less than 6 times (in each case on the first and second diagram). The data was created with a few Ruby scripts. The diagrams were then made with LibreOffice. I evaluated the data too well as I could. However, I do not guarantee correctness.

11-06-2020


TencentCloud
TENCENT-CN
ALISOFT
CHINANET-SH
unknown
CHINANET-GD
CHINANET-JS
CHINANET-SD
Xiaoniaoyun
TEAMSUN
UNICOM-SD
others

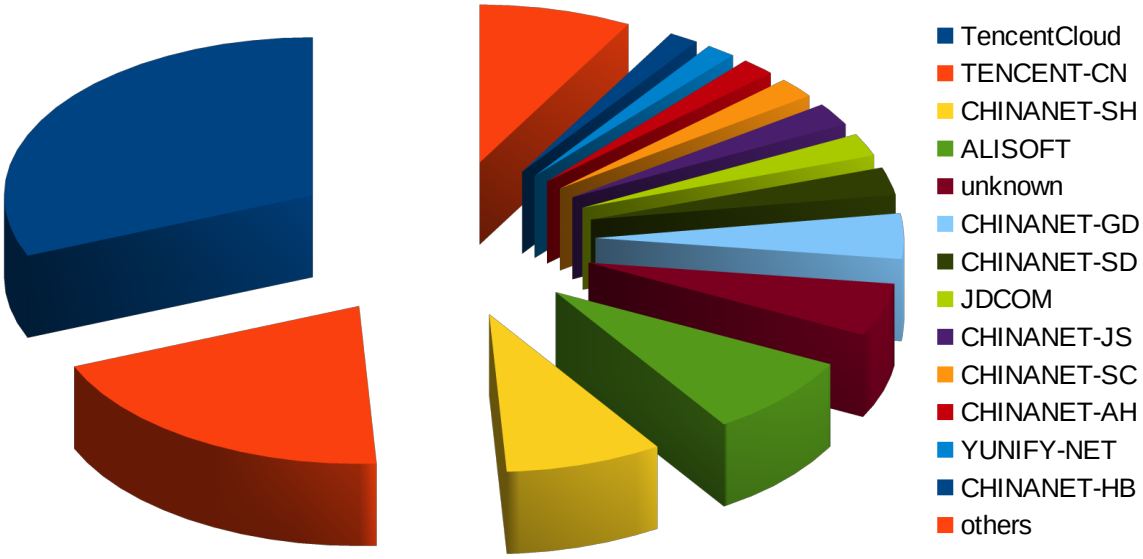

others
118.24.x.x
106.53.x.x
180.163.x.x
193.112.x.x
129.204.x.x
49.233.x.x
118.89.x.x
103.45.x.x
49.235.x.x
101.227.x.x
140.246.x.x
134.175.x.x
122.14.x.x
106.52.x.x

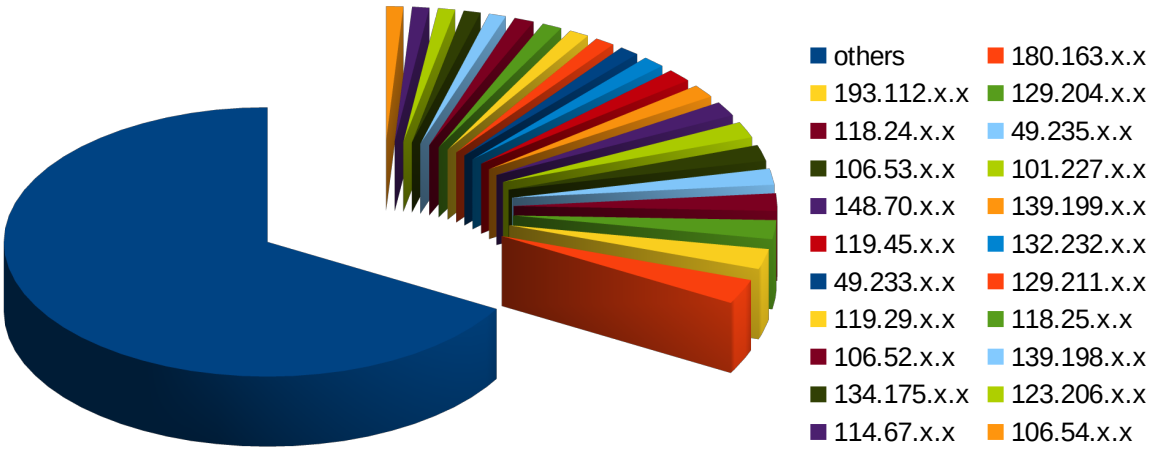
12-06-2020


TencentCloud
TENCENT-CN
ALISOFT
CHINANET-SH
CHINANET-GD
CHINANET-SD
CHINANET-SC
CHINANET-JS
others


others
180.163.x.x
148.70.x.x
129.204.x.x
118.24.x.x
49.233.x.x
134.175.x.x
116.31.x.x
106.53.x.x
49.235.x.x
182.42.x.x
182.254.x.x
139.199.x.x
119.45.x.x
106.55.x.x

13-06-2020





Sources:

- http://zzz.i2p/topics/2908-lots-of-chinese-routers
- https://i2p-metrics.np-tokumei.net/router-distribution
- https://twitter.com/NP_tokumei/status/1271204254951202819
- Discussions on Discord and in the I2P IRC.